网络空间威胁对抗与态势感知研讨会
暨 第六届安天网络安全冬训营

从“绿斑”和“方程式”组织看不同等级威胁行为体的攻击能力

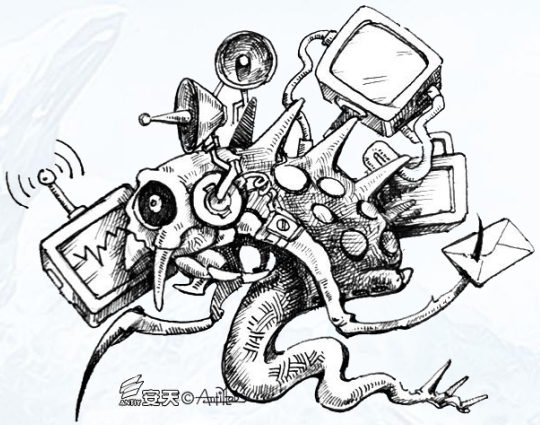
安天应急处理中心

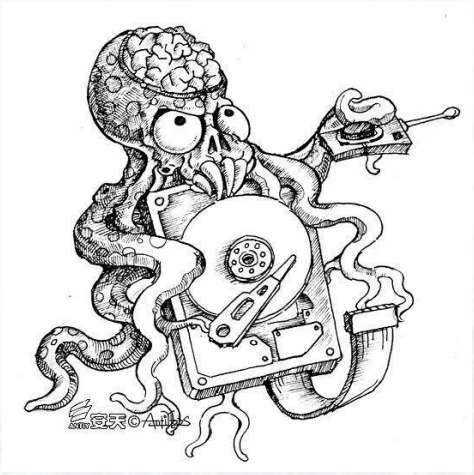
战术型态势感知指控积极防御
协同响应猎杀威胁运行实战化

铁流鏖戰

提纲

- 绿斑组织攻击行动回顾
- 方程式组织攻击EastNets行动复盘
- 不同等级威胁行为体攻击能力横向对比





分层级的威胁框架——认知不同层级的威胁

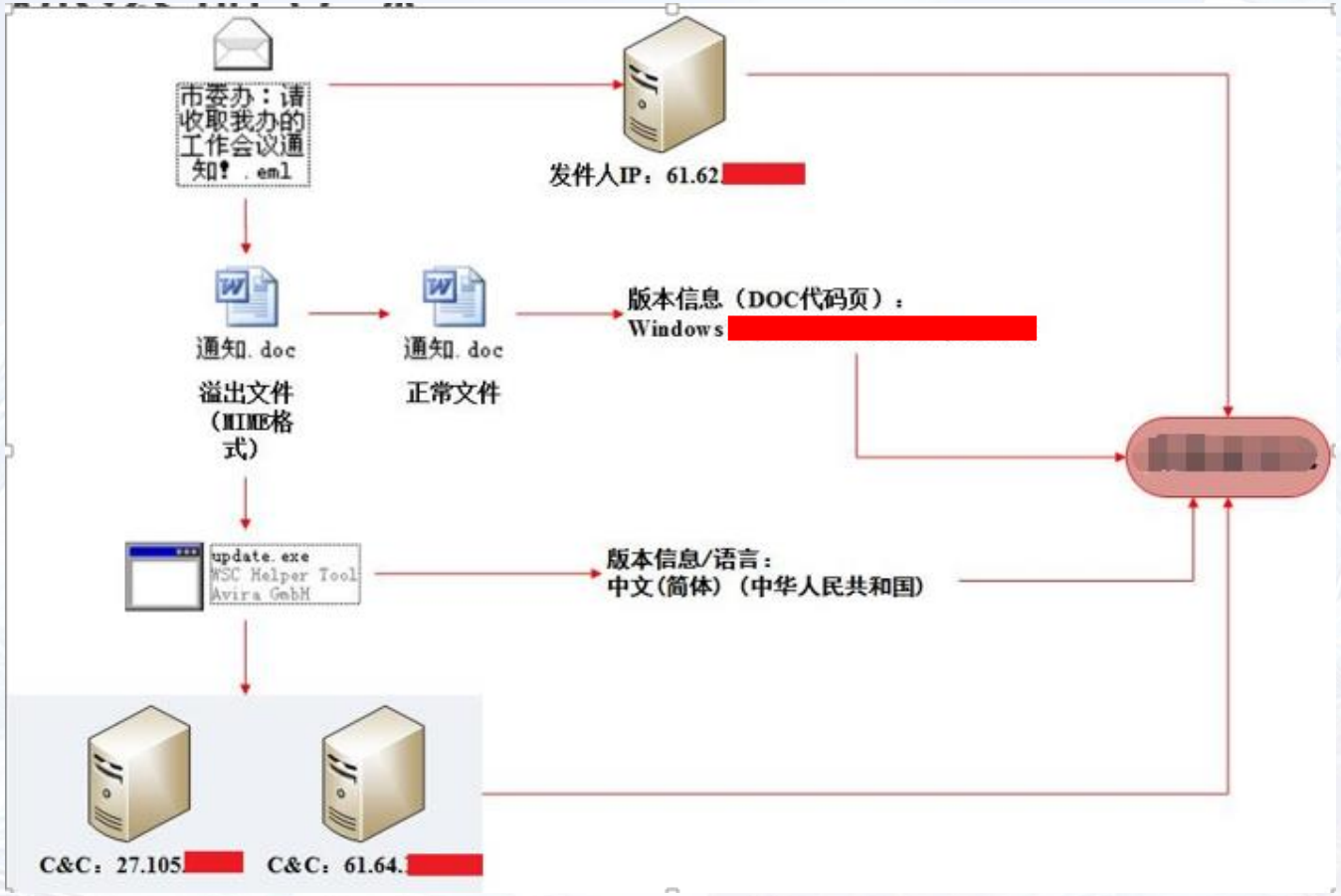
01 绿斑组织攻击行动回顾

见微知著

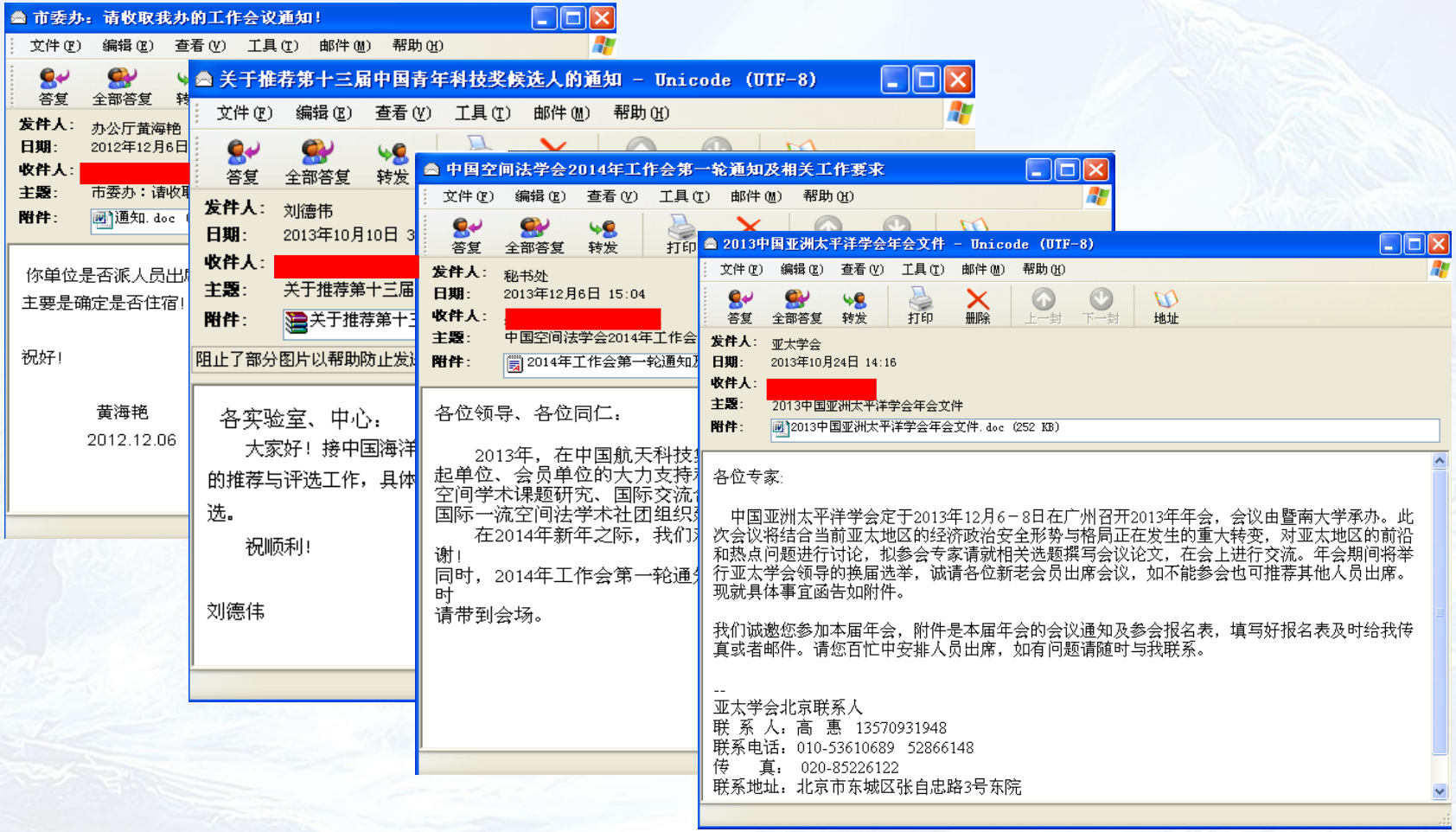
“绿斑”组织概况

- 活跃时间
  - 2007年我们发现来自该地区的攻击，由于时间间隔较远目前不确定与“绿斑” 存在确定联系。
  - 2011年-2014年，该组织主要活跃期，期间可能攻击了几十个相关目标，其攻击目的为窃取大量的政治、军事和科研机密。
  - 2017年末至2018年中旬，该组织再次筹备攻击武器和基础设施继续活跃。
- 攻击目标及组织背景
  - 通过多事件间的横向对比和单事件中纵向分析，我们认为攻击目标是我方政府机构和军事、海事相关机构
  - 在分析中我们发现，部分样本的开发者可能使用的是繁体中文操作系统，在我们跟踪的IP中，有90%以上的来自某地区
- 攻击载体
  - 封原始EML文件
  - 文档格式漏洞文件和伪装office的PE文件
  - 后门程序（十几种类型）
  - C&C域名和大量的IP地址
  - 攻击武器针对Windows、Linux系统

绿斑—典型事件攻击过程


市委办：请收取我办的工作会议通知！.eml
发件人IP：61.62
通知.doc
溢出文件（MIME格式）
通知.doc
正常文件
版本信息（DOC代码页）：
Windows
update.exe
WSC Helper Tool
Avira GmbH
版本信息/语言：
中文(简体)（中华人民共和国）
C&C：27.105
C&C：61.64.

攻击手法——鱼叉式钓鱼邮件

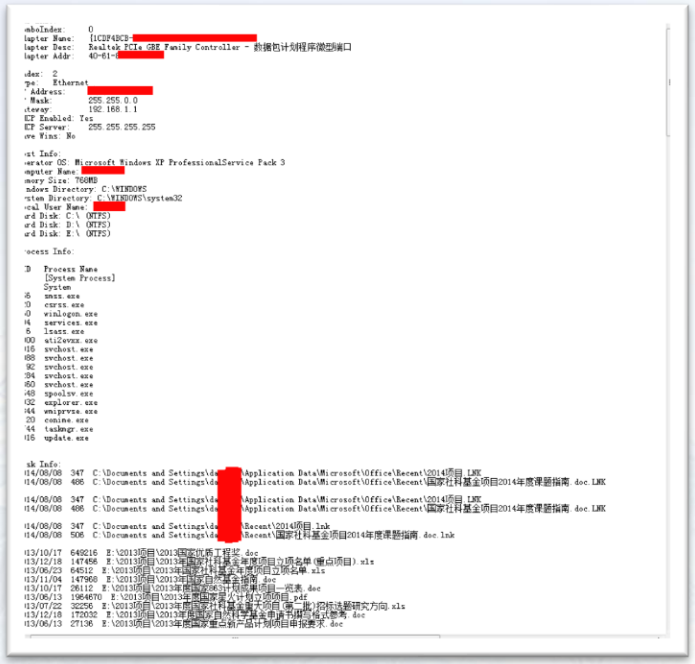


针对目标——政府、科技和海事领域

部分恶意文档或PE相关原始文件名	部分释放的文档文件相关原始文件名
通知.doc	通知.doc
国家测绘地理信息局2012年第5号公告.doc	国家测绘地理信息局2012年第5号公告.doc
两会重要发布报告.doc 海底观测网试验系统项目第四次工作会会议纪要.doc 安全重大问题咨询会议纪要0206.doc	两会重要发布报告.doc
重要通知.doc	重要通知.doc
未知	234.doc
2013中国亚洲太平洋学会年会文件.doc 2014年工作会第一轮通知及相关工作要求V2.0.doc	123.doc
关于推荐第十三届中国青年科技奖候选人的通知.exe	关于推荐第十三届中国青年科技奖候选人的通知.doc
TC无人直升机.exe	TC无人直升机.doc
会议通知.doc	1007.doc
中国海洋发展与指挥控制论坛文件.doc	研讨会.doc
2014年学术年会征集论文.exe	data.doc
全文纪录.doc	data.doc
未知	form.doc
未知	科研项目经费自查.xls
会议记录.doc	Wor.doc
应急会议通知.doc	Wor.doc
调研材料.docx	调研材料.docx
关于对互联网上存储处理传输涉密信息和违规定密问题检查工作的要求.exe	关于对互联网上存储处理传输涉密信息和违规定密问题检查工作的要求.doc
2014年度执法计划.doc	Wor.doc
中国国际问题研究学会推荐表.exe	中国国际问题研究学会推荐表.doc
调研报告修改稿0305.doc	南海危局与台湾困境.doc 申报中心项目根据专家初审意见作的修改.doc（VT）
未知	data.doc
未知	前期.doc
舆情报告.exe	舆情报告.doc
校友信息--请核实个人联系电话... 电话_docx.exe	校友信息征集启事.doc

攻击目的——主机信息获取及浏览器账号密码获取

获取被攻击主机信息：硬件信息、系统信息、网络信息、进程信息、关键字文件列表



获取IE自动保存的邮箱账户密码和对应网址，对IE6和IE6以上的版本采取不同的方法。

攻击目的——文档文件获取

- 样本收集*.doc*、*.xls*、*.ppt*等文档文件（案例6只收集网络磁盘、U盘、CDROM中的文件，案例7-8则收集全盘文件）
- 只收集半年内修改过的文档文件并使用RAR打包
- 以日期加磁盘卷序列号命名（案例6以磁盘卷序列号命名），后缀名和压缩包密码各不相同。

```
memset(&StartupInfo, 0, 0x44u);
StartupInfo.cb = 68;
if ( CreateProcessA(0, &CommandLine, 0, 0, 0, 134217728u, 0, 0, &StartupInfo, &ProcessInformation) == 1 )
{
  CloseHandle(ProcessInformation.hProcess);
  CloseHandle(ProcessInformation.hThread);
}
v42 = strlen(&v79);
strncat(&v72, &v79, v42);
v43 = strlen("*.ppt*");
strncat(&v72, "*.ppt*", v43);
if ( CreateProcessA(0, &v72, 0, 0, 0, 0x8000000u, 0, 0, &StartupInfo, &ProcessInformation) == 1 )
{
  CloseHandle(ProcessInformation.hProcess);
  CloseHandle(ProcessInformation.hThread);
}
v44 = strlen(&v79);
strncat(&v71, &v79, v44);
v45 = strlen("*.wps*");
strncat(&v71, "*.wps*", v45);
if ( CreateProcessA(0, &v71, 0, 0, 0, 0x8000000u, 0, 0, &StartupInfo, &ProcessInformation) == 1 )
{
  CloseHandle(ProcessInformation.hProcess);
  CloseHandle(ProcessInformation.hThread);
}
v46 = strlen(&v79);
strncat(&v70, &v79, v46);
v47 = strlen("*.xls*");
strncat(&v70, "*.xls*", v47);
```

攻击目的——关键字资料收集

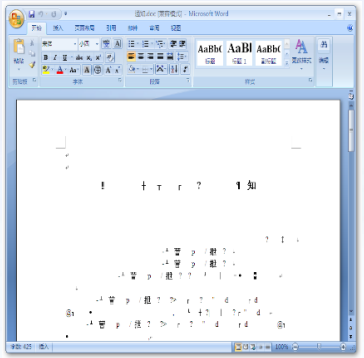
- 样本根据各自的配置，收集全盘包含指定关键字的文件路径、收集C盘Program Files目录下的EXE文件，将收集到的文件路径信息同样记录在Application Data\Microsoft\Windows\Profiles.log。

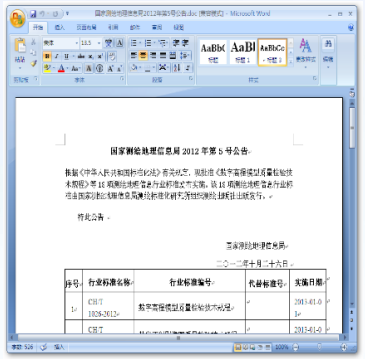
```
if ( *driver != 65 )
{
  collect_profiles(driver, "201", v102, v104, v105, v106);
  collect_profiles(driver, "军", v84, v85, v102, v104);
  collect_profiles(driver, "项", v86, v87, v88, v89);
}
```

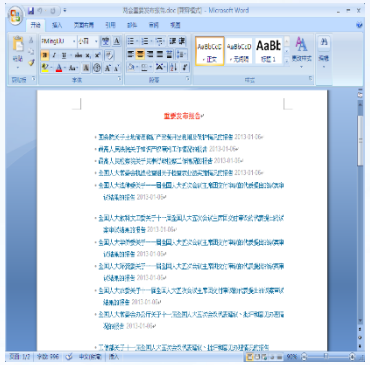
- 根据目前已捕获样本，我们总结出该系列样本关注的关键字，各个样本都是选取下列关键字中的三个，根据关键字对攻击目标进行收集操作。

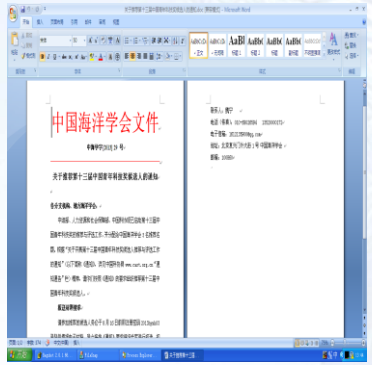
201、申、项、报、告、部、战、军、航、对X、国际、无人、报告工作、规划、合作、机场、基地、军事、内部、铁路、运输

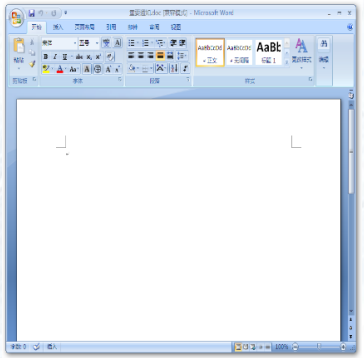
攻击组织使用的掩饰文档

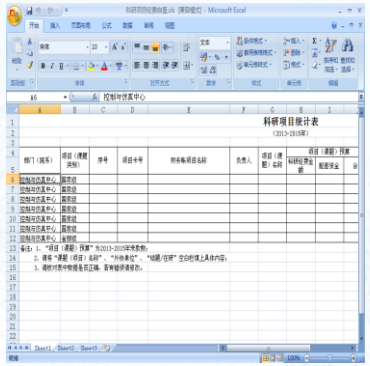


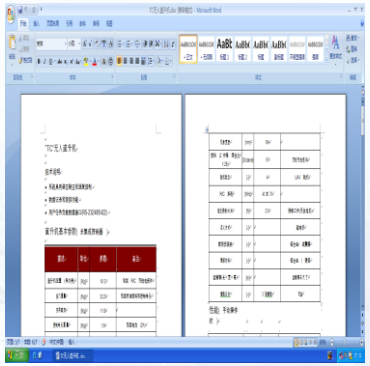








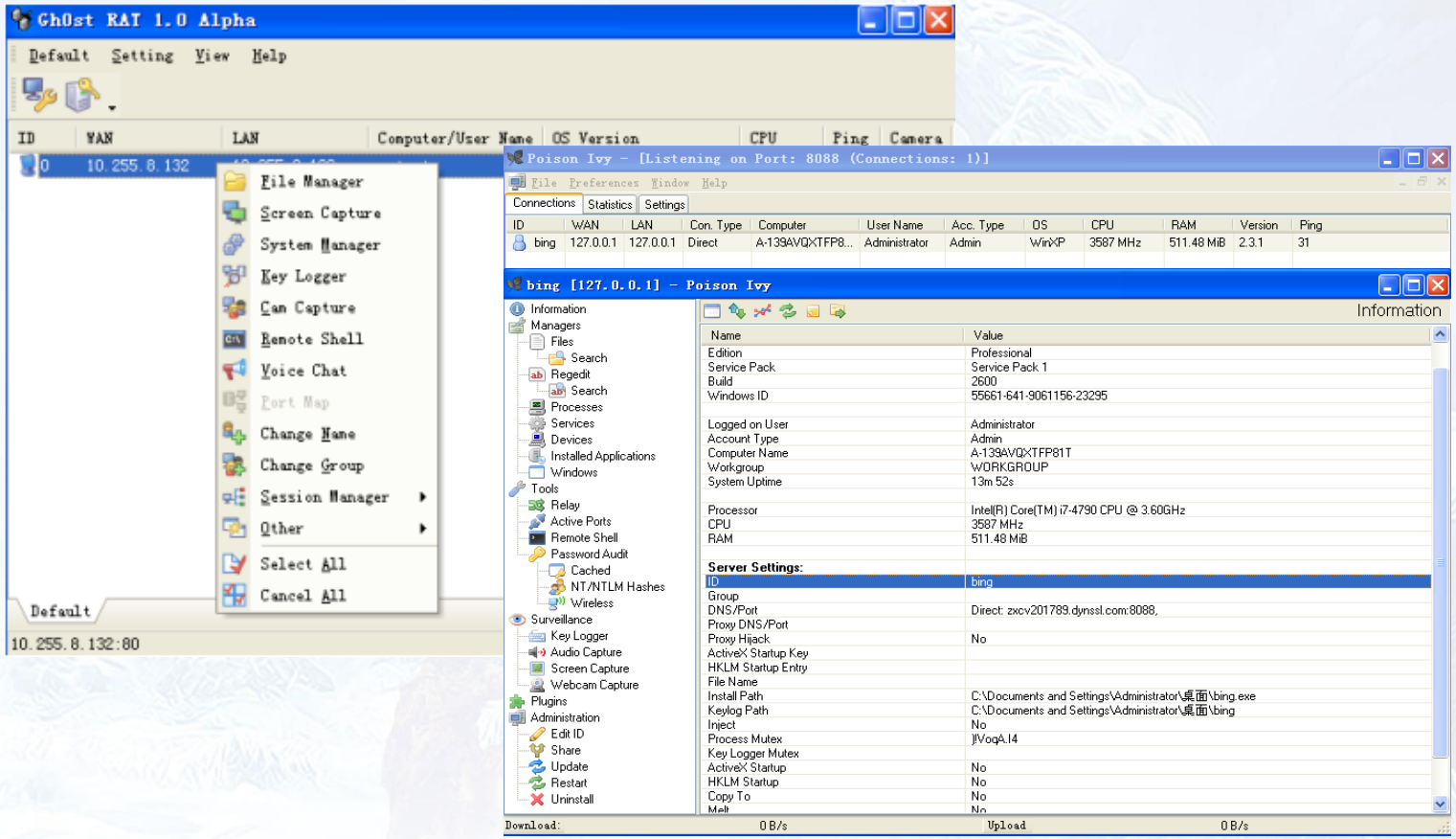




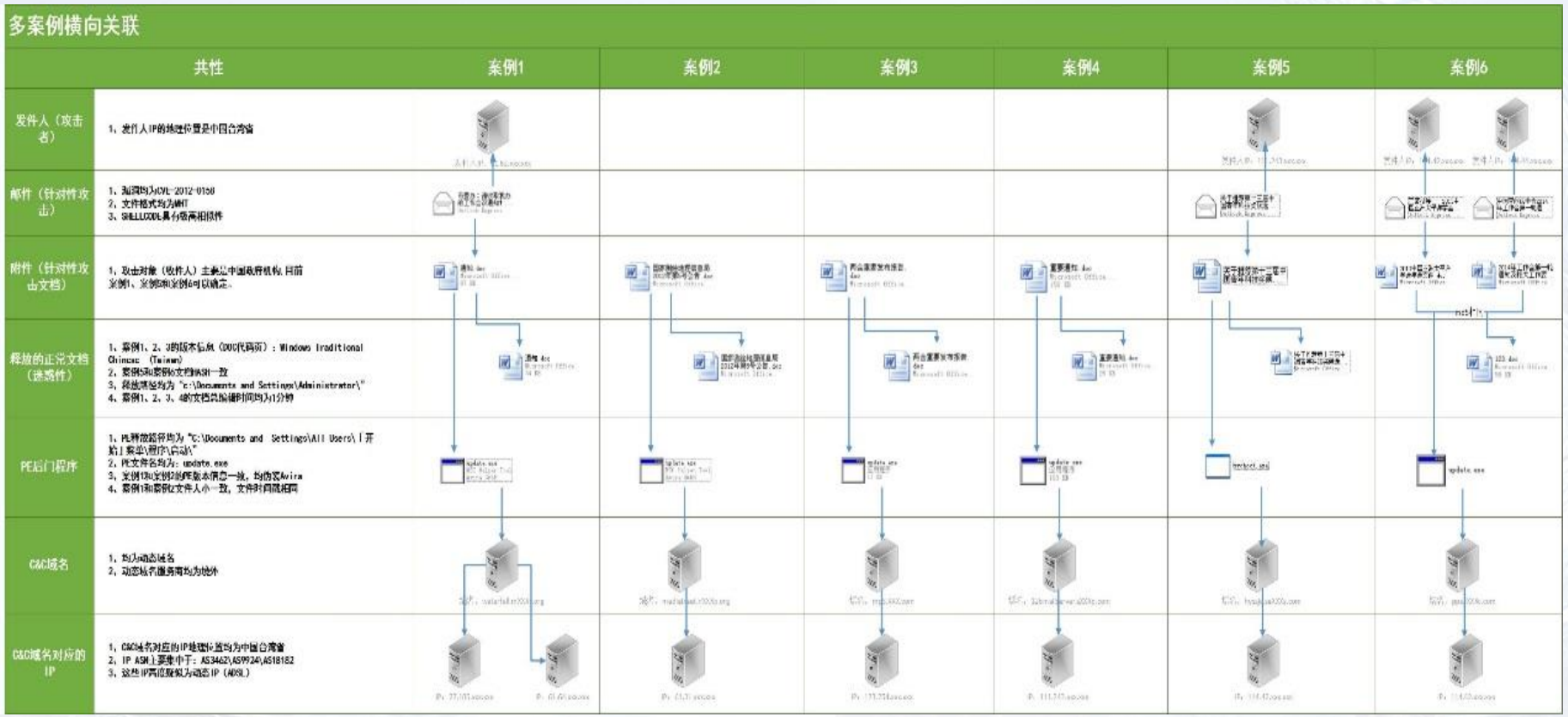
载荷武器——漏洞文档/RAT

- CVE-2012-0158(1DAY改进)
- CVE-2014-4144(0DAY)
- CVE-2017-8759(1DAY)

- Gh0st
- PI
- ZxShell修改版
- kbox
- httpbot



多案例横向关联


多案例横向关联
共性
案例1
案例2
案例3
案例4
案例5
案例6
发件人（攻击者）
1、发件人IP的地理位置是中国台湾省
邮件（针对性攻击）
1、漏洞均为CVE-2012-0158
2、文件格式均为RTF
3、SHELL32.DLL具有极高相似性
附件（针对性攻击文档）
1、攻击对象（收件人）主要是中国政府机构 目前案例1、案例2和案例6可以确定。
释放的正常文档（迷惑性）
1、案例1、2、3的版本信息（DOS代码页）：Windows Traditional Chinese (Taiwan)
2、案例5和案例6文档格式相一致
3、释放路径均为 "c:\Documents and Settings\Administrator\"
4、案例1、2、3、4的文档创建时间均为1分钟
PE后门程序
1、PE释放路径均为 "C:\Documents and Settings\All Users\「开始」菜单\程序\启动\"
2、PE文件名均为：update.exe
3、案例1和案例2的PE版本信息一致，均伪装Avira
4、案例1和案例2文件大小一致，文件时间戳相同
C&C域名
1、均为动态域名
2、动态域名服务商均为境外
C&C域名对应的IP
1、C&C域名对应的IP地理位置均为中国台湾省
2、IP ASN上要集中于：AS3462\AS9924\AS18182
3、这些IP两近频繁为动态IP（ADSL）

RAT PI和 RAT ZxShell 配置之间的关系

- 通过对RAT相关样本分析，我们得出其上线ID和密码。我们可以看到其中有多组样本均采用了同样的ID和密码，（例，ID：90518，密码：kkbox55）。

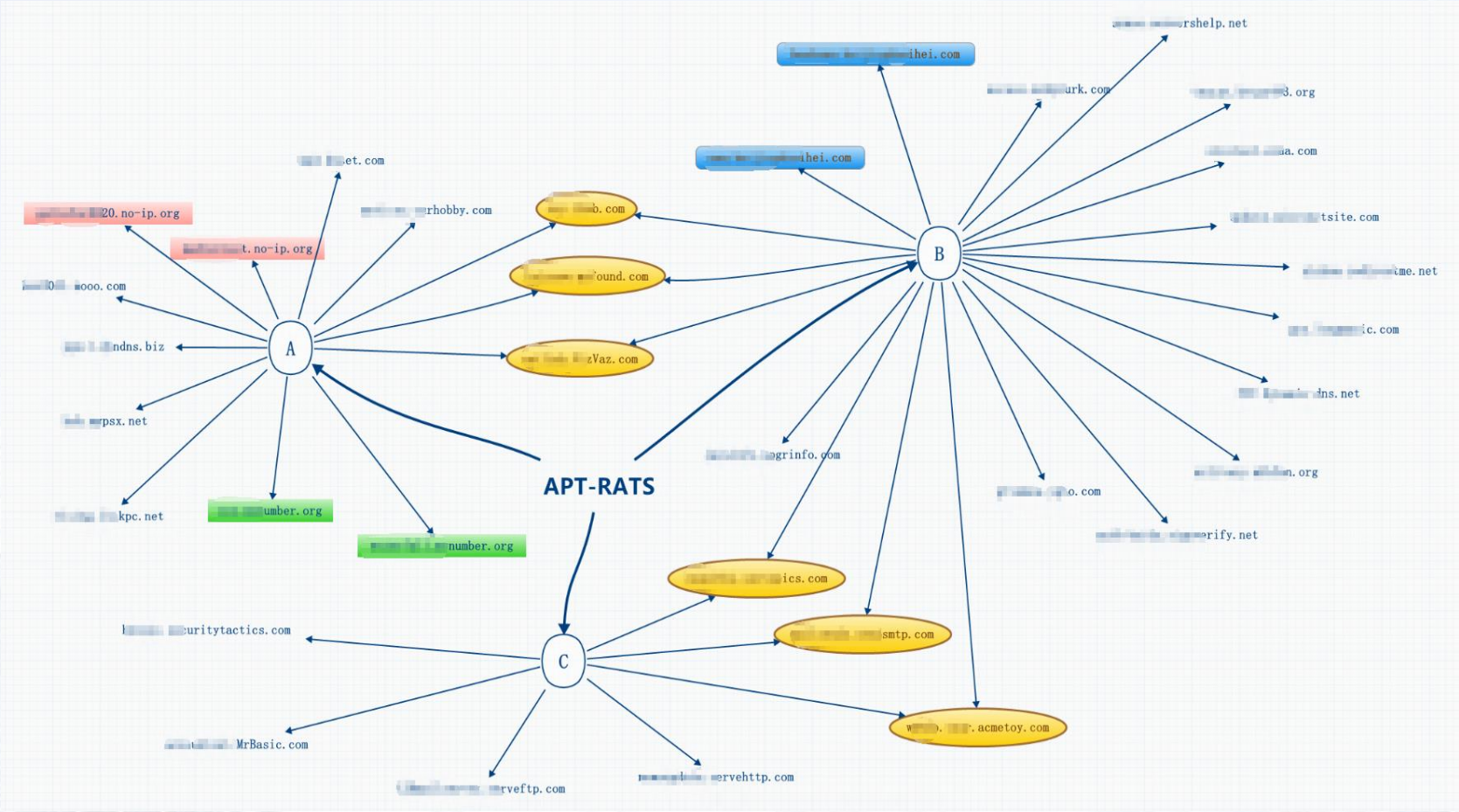
ID	密码
14	0926
14	8613
90518	kkbox55
90518	kkbox55
zhan	ftp1234
zhan2	ftp1234
120707	hook32wins
[redacted]m	hook32wins
avex	admin
w6U900	admin
motices	ps135790
1013	@1234@
wu	45002931
bs21	b53s

RAT A

上线密码	压缩密码、后缀名
admin	fish1111、.bin
8613	8613、.ttf
8613	8613、.mib
95279527	95279527、.bin
95279527	asusgo、.bin
goapple	goapple、.bin
1507	1507、.bin
cma1998	kvkv2012、.bin
iphone5	abcd123++、.bin
success	qwer4321、.bin
hook32wins	hook32wins2w、.tmp
987	zxcvasdf、.ocx
ftp533	ftp1234、.dat
Qwer!2#$	zxcvfdsa、.bin
qwer1234	kano918、.bin
qwer1234	dank1234、.bin
qwer1234	ftp1234、.bin
661566	661566、.bin

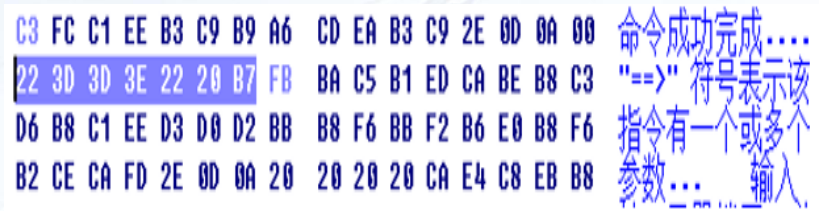
RAT B

RAT A/B/C之间C&C关系

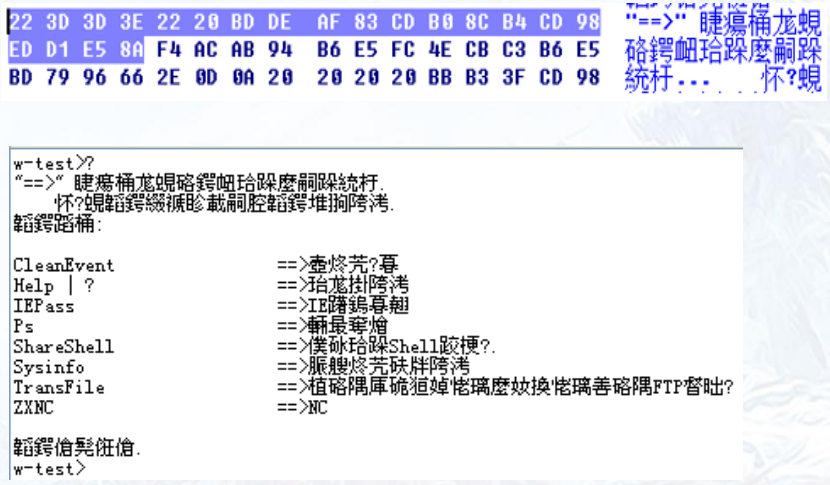


编码失误

- 在某案例样本中，指令的帮助提示为正常中文，而案例8样本是乱码，经过分析，发现新样本其实对这部分中文是BIG5编码（一种繁体字编码），而在编译程序时候却将这部分转换为GB2312编码，导致显示乱码。



中文简体原版提示



编码错误造成乱码

组织特点及背景

- 通过分析我们确定本次幕后的攻击者或攻击组织可能来自某地区。

攻击目标	发件人邮件地址、邮件标题和内容精心构造，以假乱真
	文件名具有敏感词语，只有相关人士才会查看
	释放的文档是有一定机密性的文件
	收集*.wps*文档文件，一般中国大陆使用 WPS 软件较多
	版本信息中文（简体）（中华人民共和国），刻意加的（中华人民共和国）
	域名伪装成中国大陆的一些软件名称
	只对中国大陆的三款安全软件有检测处理
	收集文件特定关键字（简体中文）的文件列表
攻击来源	邮件发件 IP 绝大多数来自某城市
	域名指向 IP 绝大多数来自某城市
	释放的文档，在不可见字符处编码显示某地区位置
	部分样本内部使用 BIG5 编码
	收集含有某地区等关键字的文件列表

02 方程式组织攻击EastNets行动复盘

盲人摸象

Windows文件夹——NSA/DS-FB攻击平台结构简析

NSA/DS-FB攻击平台结构简析							
DanderSpritz/支持命令					fuzzbunch		
平台管理	进程操作	文件操作	kisu模块存储库	网络操作	内置漏洞（exploits文件夹）	漏洞扫描工具集（touches文件夹）	后渗透阶段载荷及插件（payloads文件夹）
commands	cprpc	checksum	kisu_fulllist	domaincontroller	Easybee 1.0.1 Mdaemon漏洞	Architouch	Doublepulsar
addresses	debug	database	kisu_addmodule	banner	Easypi 3.1.0 IBM Lotus漏洞	Domaintouch	Jobadd
aliases	handles	copy	kisu_config	arp	Eclipsedwing 1.5.2 MS08－067	Eclipsedwingtouch	Jobdelete
activedirectory	hide	copyget	kisu_connect	keepalive	Educatedscholar 1.0.0 MS09－050	Educatedscholartouch	Joblist
available	debugload	delete	kisu_loadmodule	nsg	Emeraldthread 3.0.0 MS10－061	Emeraldthreadtouch	Pcdlllauncher
cd	injectdll	gangsterthief	kisu_processload	packetredirect	Emphasismine 3.4.0 IBM Lotus Domino漏洞	Erraticgophertouch	Processlist
freeplugin	processconnections	mkdir	kisu_readmodule	nameserverlookup	Englishmansdentist 1.2.0 OUTLOOK EXCHANGE漏洞	Esteemaudittouch	Regdelete
frzlinks	processes	move	kisu_survey	netmap	Erraticgopher 1.0.1 SMB漏洞	Explodingcantouch	Regenum
frzroutes	processinfo	strings	kisu_uninstall	knock	Eskimoroll 1.1.1 MS14－068	Iistouch	Regread
frzaddress	processmemory	systempaths	kisu_upgrade	ping	Esteemaudit 2.1.0 RDP漏洞	Namedpipetouch	Regwrite
break	processmodify	rmdir	kisu_usebh	portmap	Eternalromance 1.4.0 SMBv1 漏洞	Printjobdelete	Rpcproxy
help	processoptions	logedit	kisu_install	randdirect	Eternalsynergy 1.0.1 SMB漏洞	Printjoblist	Smbdelete
hour	processsuspend	filetype	kisu_list	route	Ewokfrenzy 2.0.0 Domino漏洞	Rpctouch	Smblist
渗透相关	远控生成连接指令	dsky脚本指令	注册表操作	硬件操作	向目标机器植入指定程序（implants文件夹）	影响较大的漏洞（specials文件夹）	
activity	pc2.2_uninstall	dsky_deletecapture	appcompat	drivers	Darkpulsar	Eternalblue/永恒之蓝	
darkskyline	pc2.2_upgrade	dsky_getcapture					
duplicatetoken	pc_connect	dsky_getfilter	performance	devicequery			
authentication	pc_install	dsky_install					
acquiretoken	pc_listen	dsky_load	registryadd	dmgz_control			
eventlogfilter	pc_master	dsky_setmaxsize					
eventlogquery	pc_pick	dsky_start	registryquery	flav_control			
eventlogsearch	pc_pick	dsky_status					
firewall	pc_status	dsky_stop	registrydelete	flav_plugins	Mofconfig	Eternalchampion	
forcelogon	pc_uninstall	dsky_uninstall					
eventlogclear	pc_upgrade	dsky_unload	appcompat_uninstall	diskspace			
getadmin	pc2.2_install	dsky_verifyinstall					
logonasuser	pc2.2_pick	dsky_verifyrunning	registryhive	drives			
.....							

SWIFT文件夹——攻击记录分析

- SWIFT文件夹中包含很多与攻击EastNets相关的证据、凭证、内部架构信息、攻击记录和攻陷信息统计等。

文件名称	内容简介
《initial_oracle_exploit.sql》	Sql脚本，用于获取系统信息，包括用户名等
《swift_msg_queries_all.sql》	Sql脚本，用于获取SWIFT金融交易信息
《JFM_Status.pptx》	JEEPFLEA_MARKET和JEEPFLEA_POWDER两个攻击任务的进展情况介绍。共4页
《Legend.pptx》	JFM_Status.pptx的最后一页。共1页
《EN Production net 01 AUG 2013.xlsx》	EastNets业务网络的调查汇总情况
《EN Production net 01 AUG 2013_kdmoore.xlsx》	EastNets业务网络的调查汇总情况
《DSquery Belgium DC.xlsx》	EastNets所涉及的比利时网络情况的查询结果
《DSquery Egypt DC.xlsx》	EastNets所涉及的埃及网络情况的查询结果
《DSquey Dubai enDCBACKUP.xlsx》	EastNets所涉及的迪拜（位于阿联酋）网络情况的查询结果
《DSquey END boxes and MX servers.xlsx》	EastNets所涉及的邮件服务器的查询结果
《DSqueyMain.xlsx》	EastNets的查询结果
《JEEPFLEA_MARKET_UAE.xlsx》	JEEPFLEA_MARKET攻击行动中与阿联酋相关的信息统计
《JEEPFLEA_MARKET_BE.xls》	JEEPFLEA_MARKET攻击行动中与比利时相关的信息统计。
《JEEPFLEA_MARKET Implants.xlsx》	JEEPFLEA_MARKET攻击中系统植入情况统计
《JEEPFLEA_MARKET Passwords V2.4.xlsx》	JEEPFLEA_MARKET密码信息汇总，（文件被加密，无法打开）
《ENSB DXB Passwords V2.4.xlsx》	EastNets服务机构与迪拜相关的密码信息汇总，（文件被加密，无法打开）
《list_of_saa_servers_8May2013.xlsx》	SAA服务器列表
《Eastnets_Huge_Map_05_13_2010.vsd》	包含多组与EastNets相关的拓扑图
《Eastnets_UAE_BE_Dec2010.vsd》	EastNets中与阿联酋和比利时相关的雇员网络拓扑图
《EN_DUBAI_ASA.vsd》	EastNets中与迪拜相关的拓扑图
《EN_DUBAI_MAIN.vsd》	与EN_DUBAI_ASA.vsd的内容相同
《ENSB UAE NW Topology V2.0.1339670413.vsd》	EastNets中与阿联酋相关的网络拓扑图
《JF_M FIN Exfil.vsd》	攻击成功后的信息回传路径图
《VPNFW_Plan.txt》	由哈萨克斯坦IP地址212.19.128.4发起攻击的记录
《DSL2opnotes.txt》	由日本IP地址133.94.1.3发起攻击的记录
《DSL1opnotes.txt》	由中国台湾IP地址163.22.20.4发起攻击的记录
《Production.txt》	由德国IP地址139.18.13.2发起攻击的记录
《Employee.txt》	由日本IP地址210.135.90.41发起攻击的记录
《Important NOTES.txt》	由日本IP地址202.145.16.4发起攻击的记录

SWIFT文件夹——当时最复杂最精心构造的攻击

- 影子经纪人在2017年4月14日公布的信息中，披露的NSA对SWIFT的攻击是截至当时最复杂以及最精心构造的攻击。

> This is by far, the most interesting release from Shadow Brokers as it does not only contain tools—but also materials describing the most complex and elaborate attack ever seen to date. A multi stages attack bypassing Cisco ASA Firewall appliances, exploiting and infecting Windows servers in order to copy Oracle databases of multiple hosts belonging to a SWIFT Service Bureau part of the internal financial system.

https://blog.comae.io/the-nsa-compromised-swift-network-50ec3000b195

SWIFT及其服务机构

- SWIFT，Society for Worldwide Interbank Financial Telecommunications,环球银行金融电信协会。
  - 总部位于比利时，提供了一个计算机网络允许超过200个国家的金融机构相互收发金融交易信息。
  - SWIFT的成员多数为银行和贸易机构。
  - SWIFT网络不直接交易现金，而是在机构账户之间，使用SWIFT码，发送付款委托书。SWIFT码又称为银行识别码，在SWIFT网络中用于交易，例如英国的巴克莱银行的代码为BARCGB22。
- SWIFT Service Bureau
  - SWIFT服务机构提供了一种最划算的访问完整SWIFT服务的方式，不需要了解SWIFT的专业知识，它相当于银行的云服务供应商。
  - 全世界范围内共有74家官方认可的SWIFT服务机构。SWIFT服务机构通过SWIFT软件和Oracle数据库来管理金融交易。

具体攻击目标——EastNets

Middle East

Provider	Country	Certification Status	Valid until	Compliant with
Allied Engineering Group	Lebanon	Standard	21 September 2017	SIP Release 2013
ABS Emirates	United Arab Emirates	Standard	13 May 2019	SIP Release 2013
EastNets	United Arab Emirates	Standard	11 April 2019	SIP Release 2013

EastNets
enabling confidentiality

Provider information:

Contact: Elsa L. Magsombol
Mail: emagsombol@eastnets.com
Phone: +971 4 3913217
Website: http://www.eastnets.com/

Standard Operational Level Information:

This Service Bureau has successfully acquired the Standard Certification level in compliance with the Terms and Conditions of the Shared Infrastructure Programme

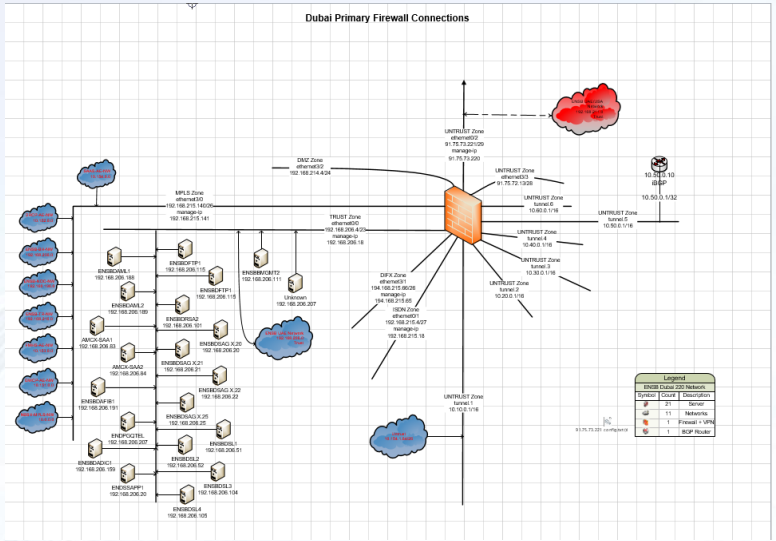
Fineksus	Turkey	Standard	2 April 2019	SIP Release 2013

JEEPFLEA_MARKET和JEEPFLEA_POWDER

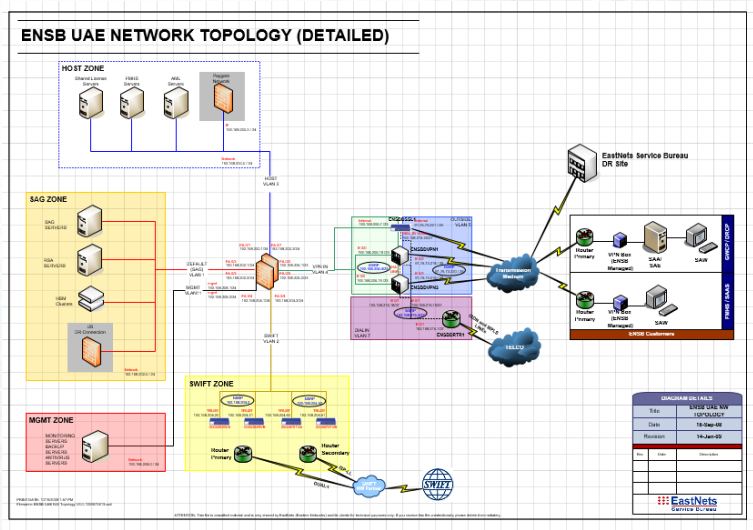
- SWIFT文件夹中的内容提及到了两个攻击事件：
- JEEPFLEA_MARKET
  - 针对EastNets的攻击，包含了网络架构、系统密码以及几千个雇员的账号。
- ~~JEEPFLEA_POWDER。~~
  - ~~是针对EastNets合作伙伴的攻击，这个合作伙伴名为BCG（Business Computer Group），位于委内瑞拉和巴拿马。（备注：此攻击的状态为无进展）。~~

网络拓扑图

攻击者渗透绘制-->



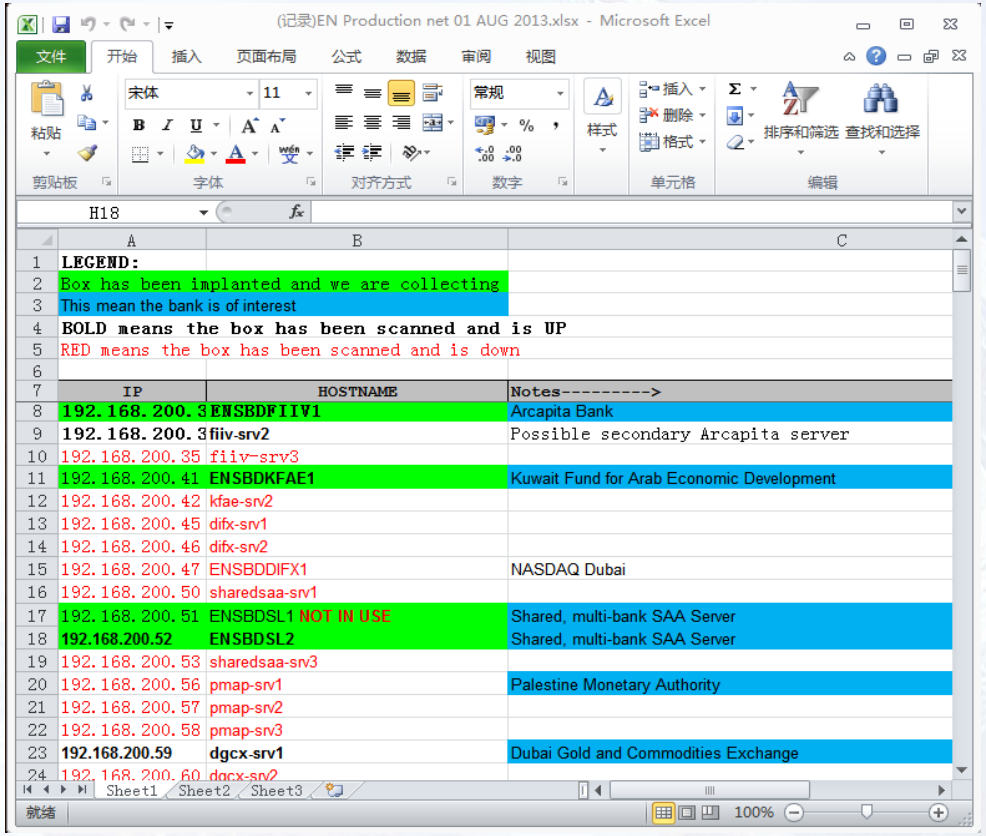
前期入侵获取——jpdm.eastnets.com-->



攻陷的设备、主机记录

- NSA披露出的信息中的关键IP
- 《EN Production net 01 AUG 2013.xlsx》
- 《EN Production net 01 AUG 2013_kdmoore.xlsx》

- 两个文件中标注出了：
  - 被成功攻击的系统（标绿）
  - 有价值的银行（标蓝）
  - 被扫描过并且正常运转的系统（字体加粗）
  - 被扫描过并且关机的系统（字体标红）



被攻陷攻击安全设备

- 被攻击的VPN设备

IP地址	名称	开放端口	MAC地址	产品型号
80.227.254.202	ENSBDVPN1	2194(ssh),8080(http),2443 (https)	0026.88ed.3d86	Juniper SSG 520M
80.227.254.203	ENSBDVPN2	2194(ssh),8080(http),2443 (https)	0010.dbff.80b0	Juniper SSG 520M
80.227.254.206	ENSBDVPN5	2194(ssh),8080(http),2443 (https)	0017.cb47.d386	Juniper SSG 520M
80.227.254.207	ENSBDVPN6	2194(ssh),8080(http),2443 (https)	0010.dbd1.8786	Juniper SSG 520M

- 被攻击的防火墙设备

IP地址	名称	开放端口	MAC地址	产品型号
192.168.206.1	ENSBDASA1	未知	00:24:97:2B:E6:8A	Cisco ASA 7.0(7)
192.168.206.4	未知	未知	未知	juniper-ssg-nsrp1

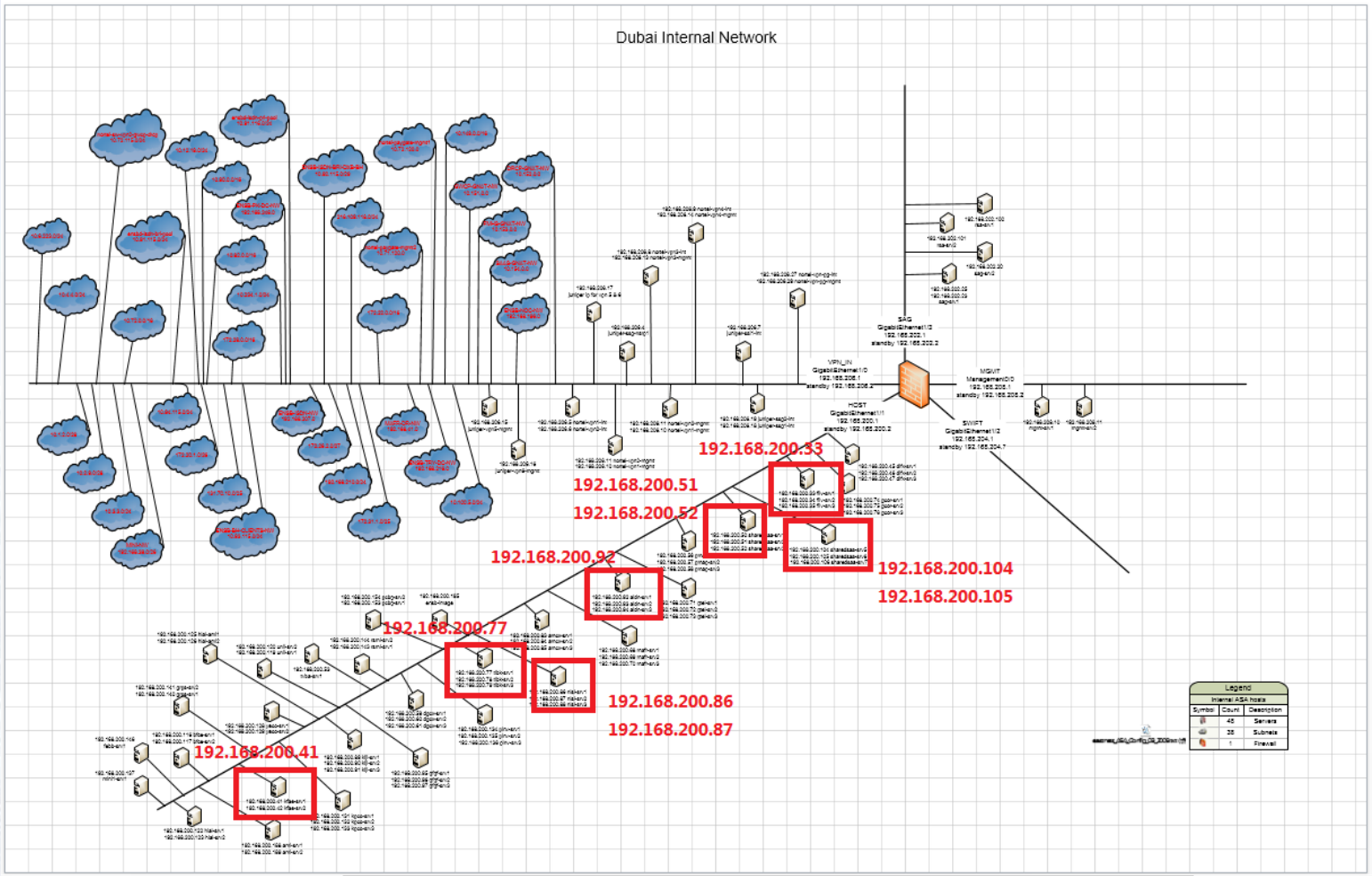
- 被攻击的管理服务器

IP地址	名称	开放端口	MAC地址	软件	操作系统	其他
192.168.206.110 (192.168.208.10 / 10.255.10.10)	ENSBDMGMT1	445, 3389	00-18-fe-7c-77-fe / 00-18-fe-7c-77-fc	Symantec Endpoint Protection 11	Windows 2008 SP 2 x86	ZB Administrator::#enSBSX10#
192.168.206.111 (192.168.208.11 / 10.255.10.11)	ENSBDMGMT2	3389	00-18-fe-7b-82-c2 / 00-18-fe-7b-82-c0	无	Windows 2008 SP 1 64位	ZB Administrator::#enSBSX10#; SNMP management host for VPN customer firewalls

被攻陷SAA业务服务器详细记录

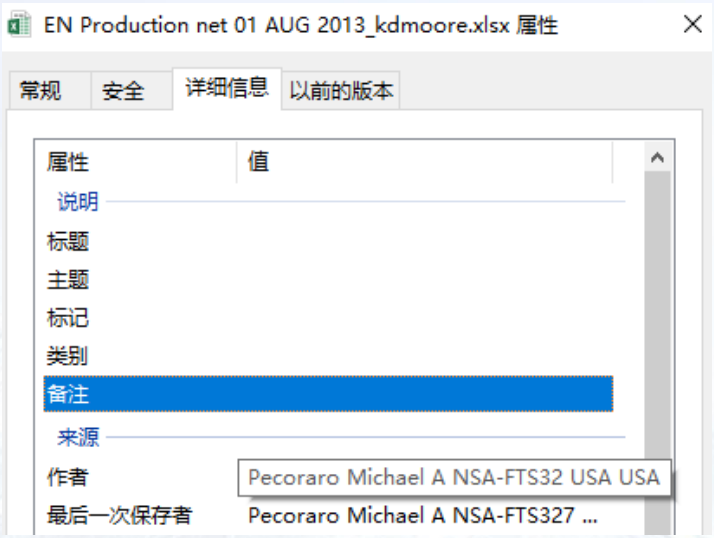
IP地址	所属机构	域名	最后一次被攻击时间	操作系统	MAC地址	PSP	登录口令	其他信息
192.168.200.33	雅卡银行，位于巴林	ENSBDFIIV1	20130808	win2008 R2 Standard	00-24-81-A7-4B-06	Symantec Endpoint Protection 11	administrator / ^enSBSX11^	Username: SAAUSER Password: AUfR6rbSeZmCwpozqqX1u6S0e Username: SAAROUSER Password: AUzYsaggdxLTEd2OhQedtJCrj
192.168.200.41	科威特阿拉伯经济发展基金	ENSBDKFAE1	20130808	Win2008 R2 sp0 64bit	00-18-fe-7a-75-c0	Symantec Endpoint Protection 11	administrator/ ^enSBSX11^	Oracle saauser/Axct5ieSPVtmoCn6XCrEB2TeP
192.168.200.51	多家银行共享的SAA服务器	ENSBDSL1	20130406	win 2008 r2 sp1 64bit	00-23-7D-EA-69-80	Symantec Endpoint Protection 11	administrator / ^enSBSX11^	Oracle saauser / Aetq9f7CQtljCHtAmstCGF64C
192.168.200.52	多家银行共享的SAA服务器	ENSBDSL2	20130808	win 2008 r2 sp1 64bit	00-23-7d-f2-f6-7c	Symantec Endpoint Protection 11	administrator / ^enSBSX11^	Oracle: saauser / Aetq9f7CQtljCHtAmstCGF64C
192.168.200.77	塔德汉国际伊斯兰银行，位于也门	ENSBDTIBK1	20130812	win2008 r2 sp0 64-bit	18-a9-05-45-3e-2c	Symantec Endpoint Protection 11	administrator / ^enSBSX11^	saauser / AHqgBrm7feLrLsuTWgk6D5aOX
192.168.200.86	努尔伊斯兰银行，位于阿联酋迪拜	ENSBDNISL1	未知	win 2008 r2 sp0 64bit	00-18-fe-7d-7f-18	Symantec Endpoint Protection 11	administrator / ^enSBSX11^	无
192.168.200.87	努尔伊斯兰银行，位于阿联酋迪拜	ENSBDNISL2	20130729	win 2008 r2 64bit	00-18-71-77-c4-38	Symantec Endpoint Protection 11	administrator / ^enSBSX11^	无
192.168.200.92	耶路撒冷开发与投资银行，位于巴勒斯坦)	ensbdaldn1.eastnets.com	20180813	win2008 R2 Standard	00-23-7d-ea-c9-98	Symantec Endpoint Protection 11	administrator / ^enSBSX11^	无
192.168.200.104	多家银行共享的SAA服务器	ensbdsl3.eastnets.com	20130813	windows 2008 R2 SP0 64bits	00-23-7d-f2-d6-08	Symantec Endpoint Protection 11	administrator / ^enSBSX11^	无
192.168.200.105	192.168.200.104 的备份机	ENSBDSL4	未知	windows 2008 R2 SP0 64bits	00-23-7D-EA-D9-88	Symantec Endpoint Protection 11	administrator / ^enSBSX11^	无

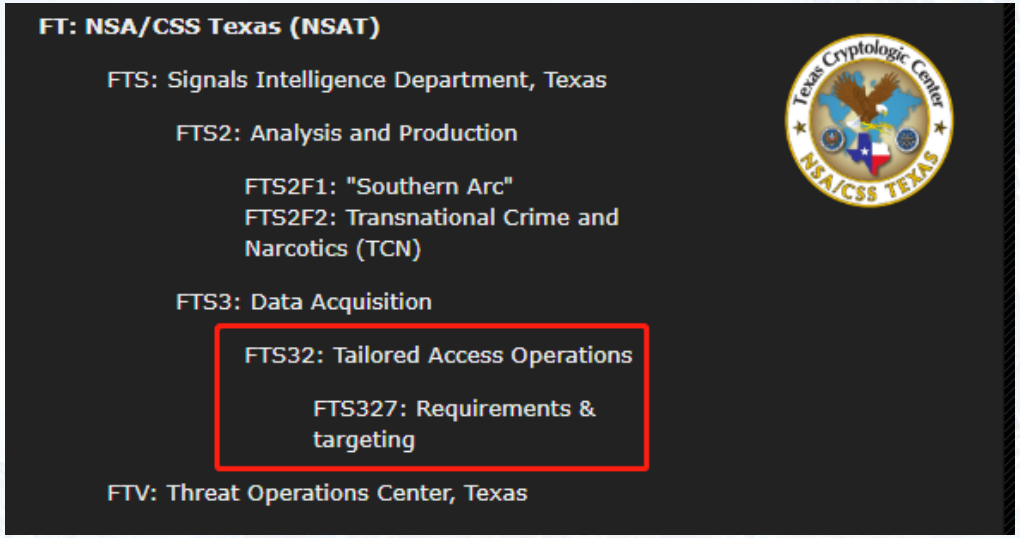
攻陷的SAA（SWIFT Alliance Access）业务服务器在网络拓扑中的位置



FTS32: Tailored Access Operations

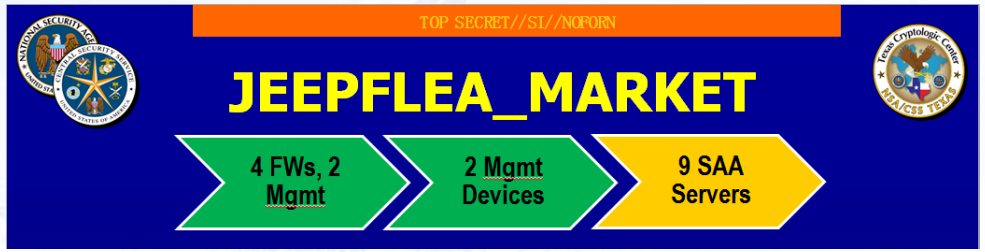
- Pecoraro Michael A NSA-FTS327 USA USA;



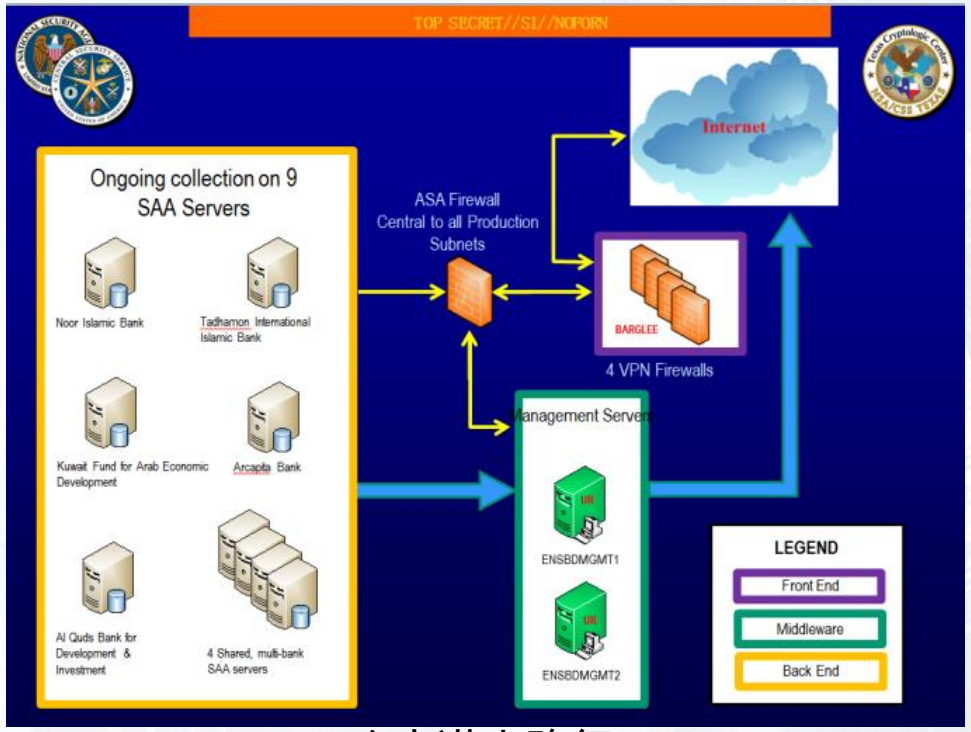


泄露PPT文件揭示的攻击路线与攻击路径

- SWIFT文件夹中有两个PPT，其中一个名为《JFM_Status.pptx》的文档中给出了攻击过程的大致描述。



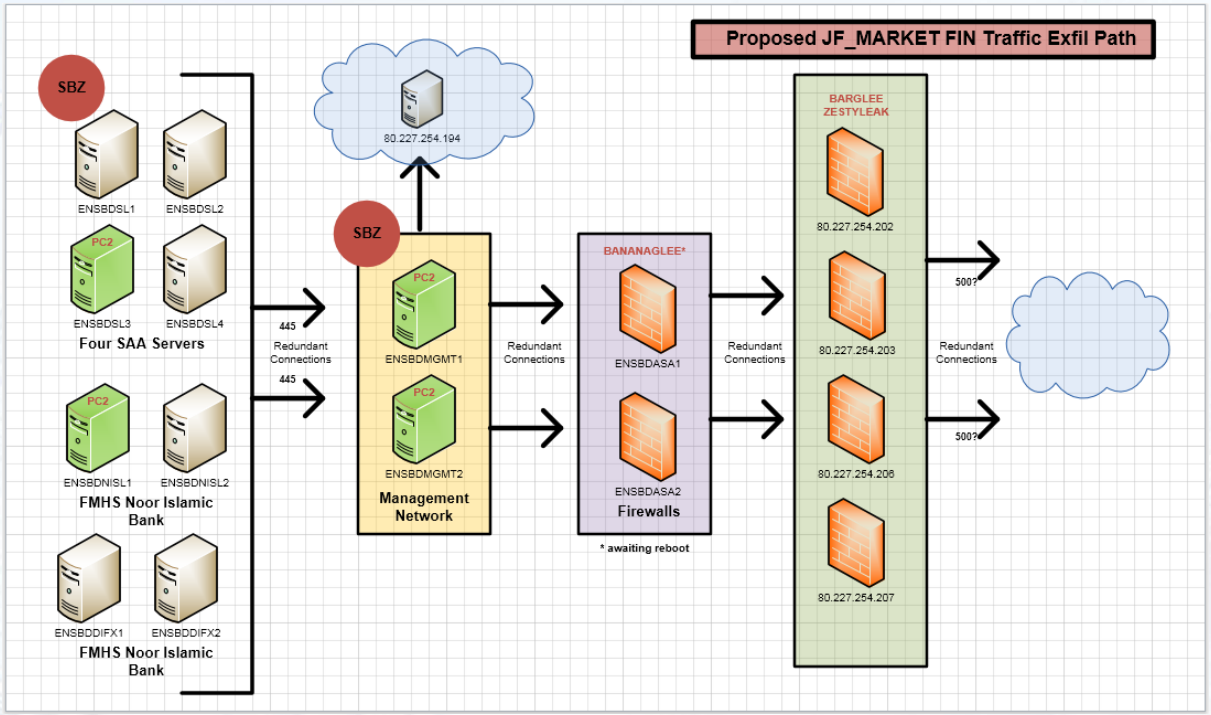
攻击路线



攻击进出路径

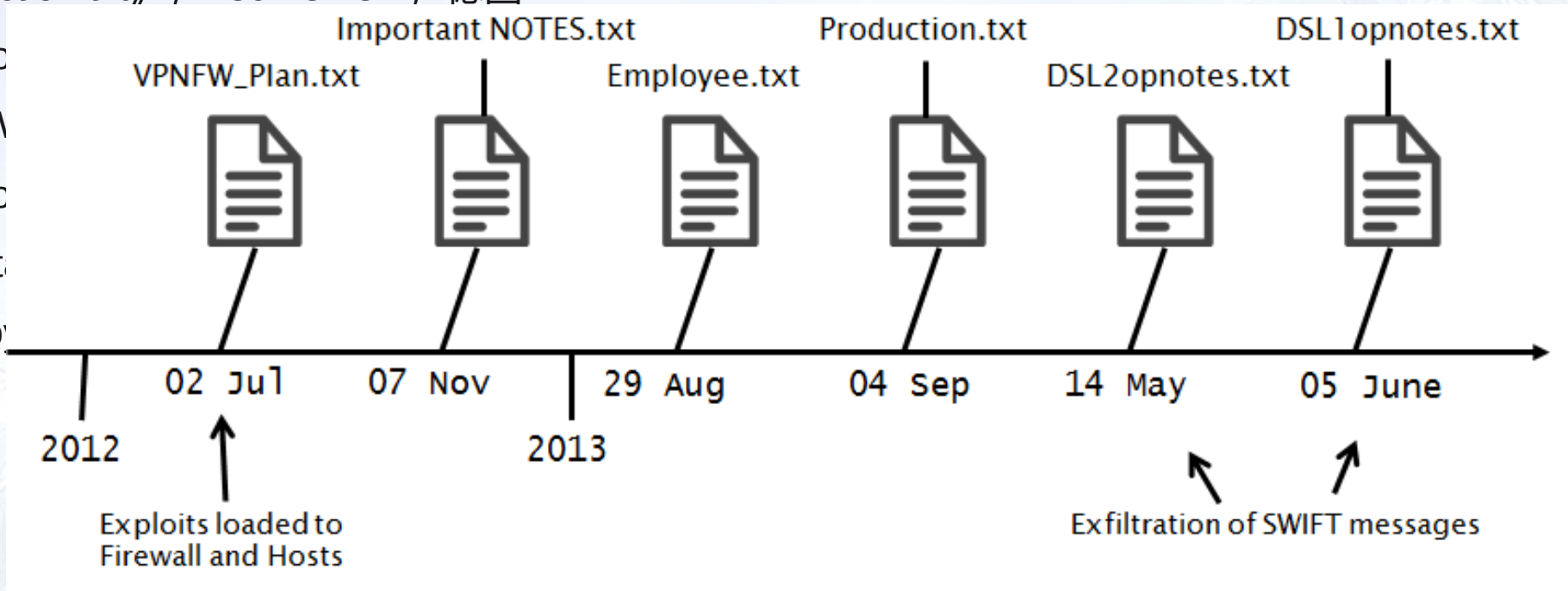
渗出路径

- SWIFT文件夹中还有一个文件，名为《JF_M FIN Exfil.vsd》，含义为攻击者撤出时的路线，与《JFM_Status.pptx》中描述的正向攻击路径几乎完全相同，只是行动的方向相反。



攻击日志、记录文件

- SWIFT文件夹中有6个文件大致描述了攻击发生的时间线
- 《Production.txt》，139.18.13.2，德国
- 《DSL1c
- 《VPNF
- 《DSL2c
- 《Import
- 《Emplo



图片来源：https://www.mwrinfosecurity.com/our-thinking/observations-on-the-eastnets-breach-operation-notes/

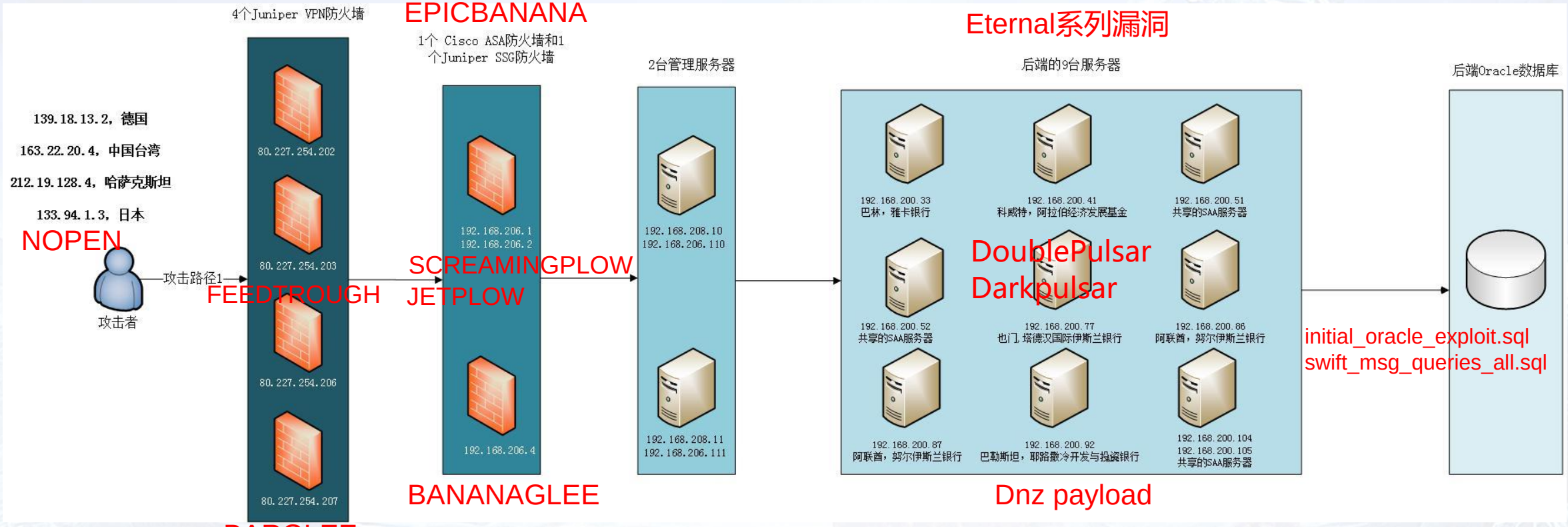
攻击工具-漏洞利用武器

工具名称	功能和针对目标
CVE-2015-7755	*针对Juniper ScreenOS的漏洞攻击武器*
EPICBANANA	针对Cisco ASA and PIX设备的漏洞攻击武器
EXTRABACON	针对Cisco ASA 设备的SNMP漏洞攻击武器
“永恒”系列漏洞攻击工具	针对windows、iis、Lotus的漏洞攻击武器
未知	针对UNIX系统主机的漏洞攻击武器

植入武器与植入物

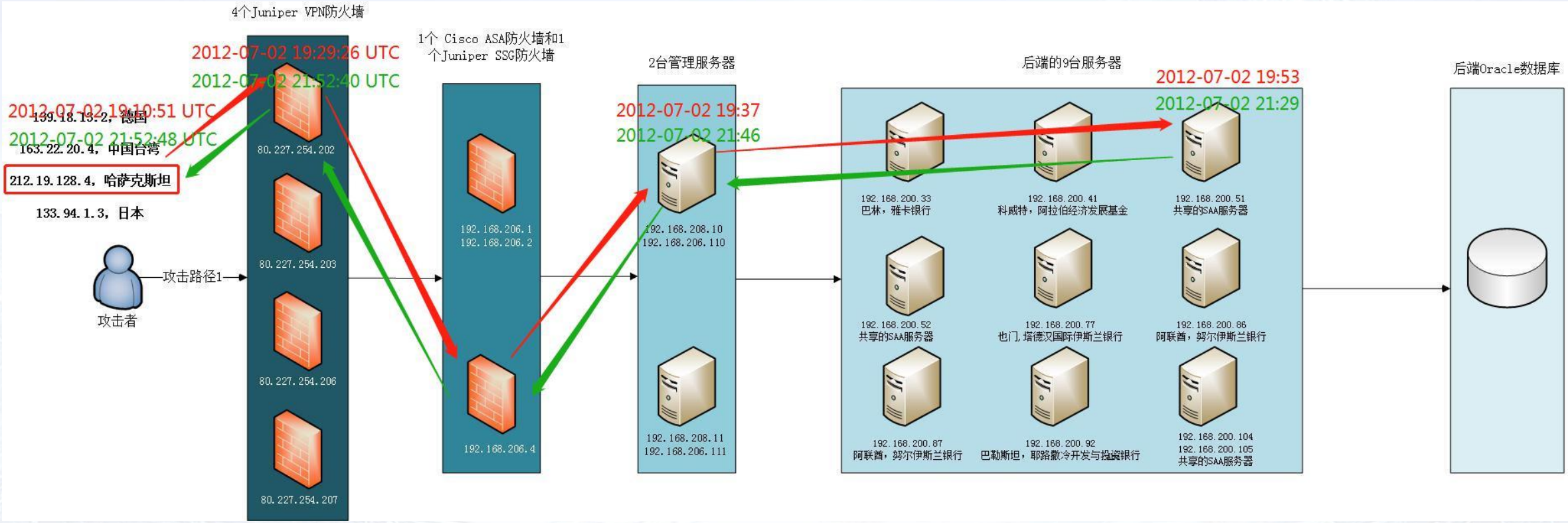
工具名称	功能介绍
JETPLOW	针对 Cisco ASA and PIX设备进行植入的武器
SCREAMINGPLOW	
BANANAGLEE	针对Cisco ASA and PIX设备的内存非持久化植入物，非持续控制工具集合（只驻留于内存中，重启后失效），目的是在获取防火墙权限后，能够实现对设备的控制。
BANANABALLOT	针对设备的BIOS的植入物（与BANANAGLEE类似）
BEECHPONY	BANANAGLEE的前身
FEEDTROUGH	针对Juniper NetScreen firewalls设备进行植入的武器
BARGLEE	Juniper NetScreen firewalls的植入物
ZESTYLEAK	
NOPEN	针对UNIX系统的后门武器
PITCHIMPAIR	Unix后门工具
INCISION	具有Rootkit功能的后门工具
DoublePulsar	针对WindowS系统的内核级植入的武器
Darkpulsar	
Dnz平台Payload	针对Windows系统的内存进程植入物

攻击工具分布图（根据泄露文件和日志分析）



典型事件——哈萨克斯坦(212.19.128.4)发起的攻击

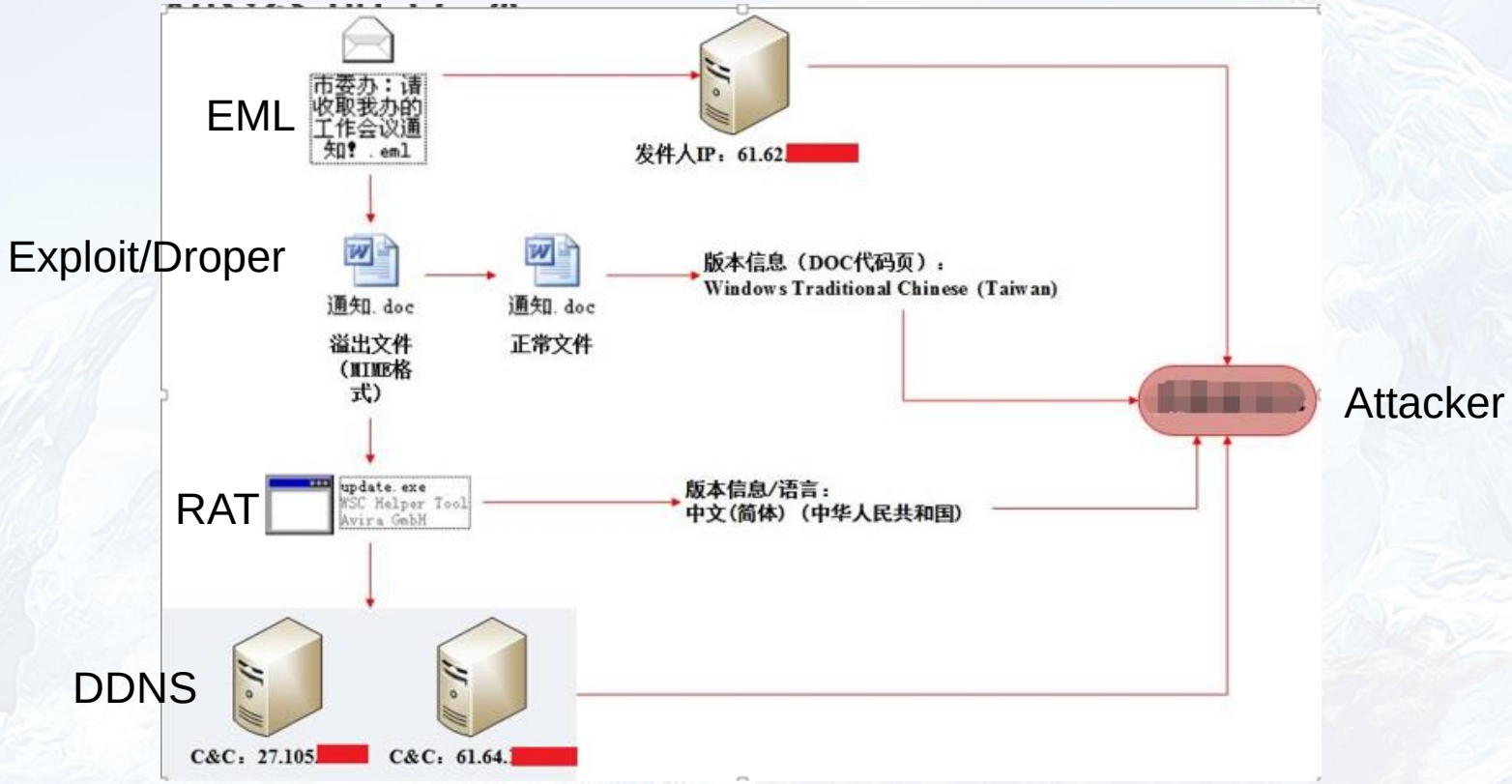
- 2012年7月2日 19点10分至21点52



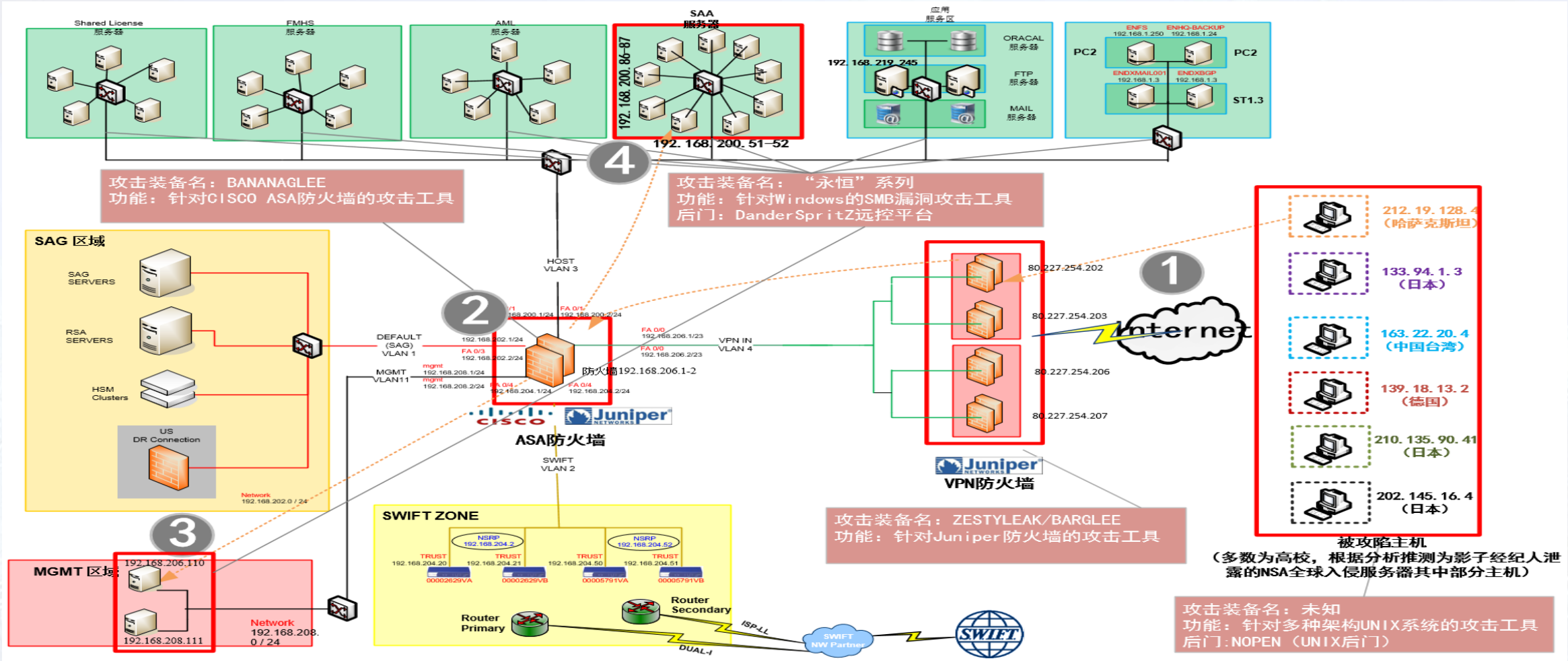
03 不同等级威胁体攻击能力横向对比

知行合一

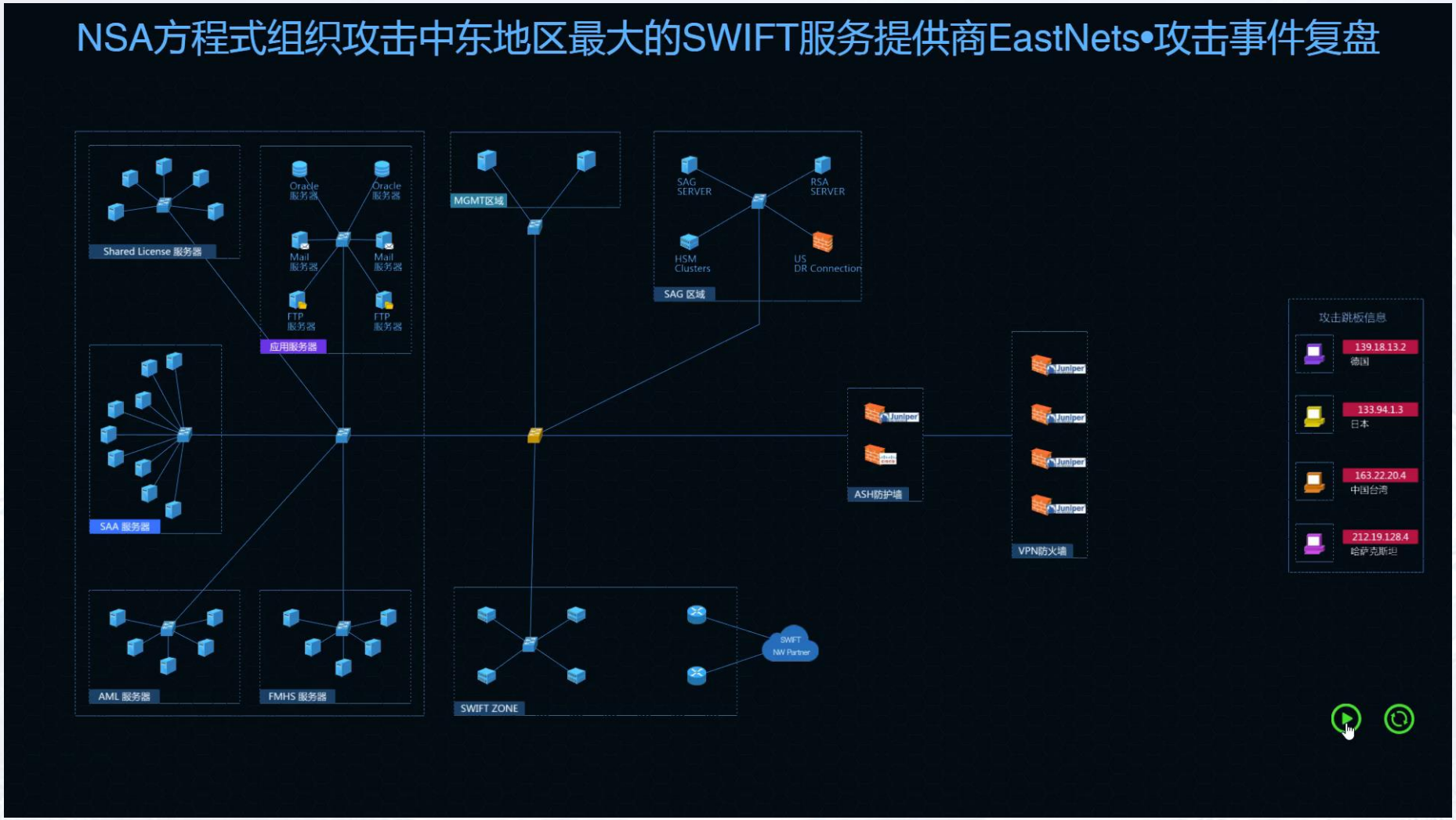
绿斑—典型事件攻击过程


EML
市委办：请收取我办的工作会议通知！.eml
发件人IP：61.62
Exploit/Droper
通知.doc
溢出文件（MIME格式）
通知.doc
正常文件
版本信息（DOC代码页）：
Windows Traditional Chinese (Taiwan)
Attacker
RAT
update.exe
WSC Helper Tool
Avira GmbH
版本信息/语言：
中文(简体)（中华人民共和国）
DDNS
C&C：27.105
C&C：61.64.

方程式入侵EastNets过程



NSA方程式组织入侵EastNets事件复盘可视化展示



知行合一构建可管理网络实现对高等级网空行为体的防御

手段和能力	方程式为代表的高级网空行为体	绿斑为代表的中等能力网空威胁行为体	高能力体现
目标入口	直接关联的系统入口，如网关、防火墙	间接被动入口，如邮件、网站、社交平台等	入口准确、稳定性好
作业方式	0day、固件植入、系统漏洞、第三方信道	以端点侧入口机为主要目标	作业目标涵盖网络上全部目标
武器来源	基本全部自研且体系化	大部分基于开源代码	难以检测、分析、查杀、阻断
攻击覆盖面	从硬件架构到系统的完整覆盖能力	主流操作系统	攻击目标全覆盖、直接攻击核心目标
横向移动	完整攻击平台、武器插件库	公开扫描、渗透工具为主	未知、定制化武器的攻击检测防护很难
信息获取	直接连接核心数据库读库	在终端主机遍历文件收集或实施监控	数据获取精准、全面
控制力	时间周期长、可复用	随机性较大、控制力弱	控制力强且持久化
回连服务器	固定IP、多数是可信机构IP	动态域名、入侵正常网站、虚拟主机为主	基础设施为攻陷的“可信”主机
通信方式	多级后门代理、公私钥加密	一层代理，通信简单加密或单向加密	流量上几乎无法破解分析

中等能力与超高能力网空威胁行为体作业模式与能力对比

网络空间威胁对抗与态势感知研讨会
暨 第六届安天网络安全冬训营

THANKS

扫码关注冬训营动态

战术型态势感知指控积极防御
协同响应猎杀威胁运行实战化

铁流鏖戰